

DOCKET FILE COPY ORIGINAL
Received or projected

FEB 19 2008

FCC Mail Room

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Washington, DC 20554

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date of execution: February 12, 2008

Name of Company covered by this certification: Coon Valley
Telecommunications, Inc.

Form 499 Filer ID: 802120

Name of Officer signing: Carol Ann Olson

Title of Officer signing: Secretary-Treasurer

I, Carol Ann Olson, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification as Exhibit 1 is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions (proceedings instituted or petitions filed by a company at either state commission, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper

Coon Valley
Telecommunications

105 Central Avenue

P. O. Box 398

Coon Valley, WI 54623-0398

Phone 608.452.3101

Fax 608.452.3100

www.coonvalleytel.com

Your local
CONNECTION
for
long distance!

CVFTC

No. of Copies made
List ABCDE

044

access to online information by individuals not authorized to view the information).

Signed Paul Am Olson

cc: Telecommunications Consumers Division, Enforcement Bureau
Best Copy and Printing, Inc.

Coon Valley Telecommunications, Inc.

**STATEMENT EXPLAINING HOW THE COMPANY'S
OPERATING PROCEDURES ENSURE COMPLIANCE
WITH THE FCC'S CPNI RULES**

I. Customer Proprietary Network Information ("CPNI")

CPNI is defined in Section 222(f) of the Communications Act as (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (except that CPNI does not include subscriber list information).

Generally, CPNI includes personal information regarding a consumer's use of his or her telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a consumer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a consumer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a consumer.

Call detail information (also known as "call records") is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

II. Use and Disclosure of CPNI Is Restricted

The Company recognizes that CPNI includes information that is personal and individually identifiable, and that privacy concerns

have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of access to it by individuals or entities inside and outside the Company.

The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Company employees and agents that may deal with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution and access. In order to be authorized to use or access the Company's CPNI, employees and agents must receive training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules).

Before an agent, independent contractor or joint venture partner may receive or be allowed to access or use the Company's CPNI, the agent's, independent contractor's or joint venture partner's agreement with the Company must contain provisions (or the Company and the agent, independent contractor or joint venture partner must enter into an additional confidentiality agreement which provides) that: (a) the agent, independent contractor or joint venture partner may use the CPNI only for the purpose for which the CPNI has been provided; (b) the agent, independent contractor or joint venture partner may not disclose or distribute the CPNI to, or allow access to the CPNI by, any other party (unless the agent, independent contractor or joint venture partner is expressly and specifically required to do so by a court order); and (c) the agent, independent contractor or joint venture partner must implement appropriate and specific safeguards acceptable to the Company to ensure the confidentiality of the Company's CPNI.

III. Protection of CPNI

1. The Company may, after receiving an appropriate written request from a customer, disclose or provide the customer's CPNI to the customer by sending it to the customer's address or record. Any and all such customer requests: (1) must be made in writing; (2) must include the customer's correct billing name and address and telephone number; (3) must specify exactly what type or types of CPNI must be disclosed or provided; (4) must specify the time period for which the CPNI must be disclosed or provided; and (5) must be signed by the customer. The Company will disclose CPNI upon affirmative written request by the customer to any person designated by the customer, but only after the Company calls the customer's telephone number of record and/or sends a notification to the customer's address of record to verify the accuracy of this request.

2. The Company will provide a customer's phone records or other CPNI to a law enforcement agency in accordance with applicable legal requirements.

3. The Company will retain all customer passwords and "shared secret" question-answer combinations in secure files that may be accessed only by authorized Company employees who need such information in order to authenticate the identity of customers requesting call detail information over the telephone.

4. Company employees will authenticate all telephone requests for CPNI in the same manner whether or not the CPNI consists of call detail information. That is, Company employees must: (a) be furnished the customer's pre-established password (or correct answers to the back-up "shared secret" combinations); (b) send the requested information to the customer's postal or electronic "address of record" (see definition above); or (c) call the customer back at the customer's "telephone number of record" (see definition above) with the requested information.

5. If a customer subscribes to multiple services offered by the Company and an affiliate, the Company is permitted to share the customer's CPNI regarding such services with its affiliate. If a customer does not subscribe to any telecommunications or non-telecommunications services offered by an affiliate, the Company is not permitted to share the customer's CPNI with the affiliate without the customer's consent pursuant to the appropriate notice and approval procedures set forth in Sections 64.2007, 64.2008 and 64.2009 of the FCC's Rules.

6. When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company may use the customer's CPNI other than call detail CPNI to assist the customer for the duration of the customer's call if the Company provides the customer with the oral notice required by Sections 64.2008(c) and 64.2008(f) of the FCC's Rules and after the Company authenticates the customer.

The Company may disclose or release call detail information to customers during customer-initiated telephone contacts only when the customer provides a pre-established password. If the customer does not provide a password, call detail information can be released only by sending it to the customer's address of record or by the carrier calling the customer at the telephone number of record. If the customer is able to provide to the Company during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call) without Company assistance, then the Company may take routine customer service actions related to such information. (However, under this circumstance, the Company may not disclose to the customer any call detail information about the customer account other than

the call detail information that the customer provides without the customer first providing a password.)

7. The Company uses, discloses, and/or permits access to CPNI in connection with Company-initiated marketing of services to which a customer does not already subscribe from the Company (out-bound marketing) only pursuant to the notice and approval procedures set forth in Sections 64.2007, 64.2008, and 64.2009 of the FCC's Rules. All proposed out-bound marketing activities are reviewed by the Company's CPNI Compliance Officer for compliance with the CPNI restrictions and requirements in the Communications Act and the FCC Rules.

8. The Company maintains appropriate paper and/or electronic records that allow its employees, independent contractors and joint venture partners to clearly establish the status of each customer's Out-out and/or Opt-In approvals (if any) prior to use of the customer's CPNI. These records include: (i) the date(s) of any and all of the customer's deemed Opt-out approvals and/or Opt-in approvals, together with the dates of any modifications or revocations of such approvals; and (ii) the type(s) of CPNI use, access, disclosure and/or distribution approved by the customer.

9. Before a customer's CPNI can be used in an out-bound marketing activity or campaign, the Company's records must be checked to determine the status of the customer's CPNI approval. Company employees, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access, accuracy or security problems they encounter with respect to these records.

If new, additional or extended approvals are necessary, the CPNI Compliance Officer will determine whether the Company's "Opt-Out CPNI Notice" or "Opt-In CPNI Notice" must be used with respect to various proposed out-bound marketing activities.

10. The CPNI Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including: (i) a description of the campaign; (ii) the specific CPNI that was used in the campaign; (iii) the date and purpose of the campaign; and (iv) what products and services were offered as part of the campaign. This record shall be maintained for a minimum of one year.

11. The Company's employees and billing agents may use CPNI to initiate, render, bill and collect for telecommunications services. The Company may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional or modified services, and its employees and agents may use such customer information (without further customer approval) to initiate and provide the services. Likewise, the Company's employees and billing agents may use customer service and calling records (without customer approval): (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

12. The Company's employees and agents may use CPNI without customer approval to protect the Company's rights or property, and to protect users and other carriers from fraudulent, abusive or illegal use of (or subscription to) the telecommunications service from which the CPNI is derived.

Because allegations and investigations of fraud, abuse and illegal use constitute very sensitive matters, any access, use, disclosure or distribution of CPNI pursuant to this Section must be expressly approved in advance and in writing by the Company's CPNI Compliance Officer.

13. The Company's employees, agents, independent contractors and joint venture partners may **NOT** use CPNI to identify or track customers who have made calls to, or received calls from, competing carriers. Nor may the Company's employees, agents, independent contractors or joint venture partners use or disclose CPNI for personal reasons or profit.

14. Company policy mandates that files containing CPNI be maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.

15. Paper files containing CPNI are kept in secure areas, and may not be used, removed, or copied in an unauthorized manner.

16. Electronic files and databases containing CPNI are maintained on computers that are not accessible from the Internet or that are on the Company's intranet behind firewalls that are regularly monitored and tested for effectiveness. In

addition, such electronic files and databases may be accessed only by authorized Company employees who have been provided a currently effective strong login ID and password (which password is periodically changed).

17. Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

18. The Company may permit its customers to establish online accounts, but must require an appropriate password to be furnished by the customer before he or she can access any CPNI in his or her online account.

19. Customers may obtain an initial or replacement password: (i) if they come in person to the Company's business office, produce a driver's license, passport or other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address; or (ii) if they call a specified Company telephone number from their telephone number of record, and then wait at that number until a Company representative calls them back and obtains correct answers to certain questions regarding their service and address.

20. The Company will notify customers immediately of certain changes in their accounts that may affect privacy or security matters.

a. The types of changes that require immediate notification include: (a) change or request for change of the customer's password; (b) change or request for change of the customer's address of record; (c) change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's responses with respect to the back-up means of authentication for lost or forgotten passwords.

b. The notice may be provided by: (a) a Company call or voicemail to the customer's telephone number of record; (b) a Company text message to the customer's telephone number of record; or (c) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

c. The notice must identify only the general type of change and must not reveal the changed information.

d. The Company employee or agent sending the notice must prepare and furnish to the CPNI Compliance Officer a memorandum containing: (a) the name, address of record, and telephone number of record of the customer notified; (b) a copy or the exact wording of the text message, written

notice, telephone message or voicemail message comprising the notice; and (c) the date and time that the notice was sent.